Discrete Mathematics 125 (1994) 123–127
North-Holland

Permutations with p^l-th roots

William W. Chernoff

Department of Mathematics and Statistics, University of New Brunswick, Fredericton, N.B. Canada E3B 5A3

Received 12 July 1991
Revised 10 December 1991

Abstract

A permutation of n objects is of cycle type $(j_1, \ldots, j_n)$ if it has j_k, $k=1, \ldots, n$, cycles of length k in its disjoint cycle decomposition. Let S_n be the symmetric group of degree n, and $d, s \in Z^+$, the set of positive integers. We enumerate the permutations in S_n of cycle type $(j_1, \ldots, j_n)$, where

$$j_k \equiv 0 \bmod s \quad \text{if } k \equiv 0 \bmod d. \tag{1}$$

For the case $d=p$, a prime number, and $s=p^l$, $l \in Z^+$, this gives the number of permutations in S_n with p^l-th roots.

1. Preliminaries

For general terminology or any undefined terms, we refer the reader to [6] or [7].

A permutation $\alpha \in S_n$ has an rth root, $r \in Z^+$, if

$$x^r = \alpha \tag{2}$$

has a solution x in S_n. In [1], Bender gives an exponential generating function for the number of permutations in S_n with rth roots. In [3], Blum gives an efficient method for computing the number of permutations in S_n with square roots (i.e. for th case $r=2$). We extend Blum's result by enumerating the permutations in S_n with p^l-th roots, where p is a prime number and $l \in Z^+$.

Often, no solution to (2) exists. The following is a simple test for the existence of a solution to (2), see [1, 5].

Let $r, k \in Z^+$ have prime decompositions: $r = p_1^{\alpha_1} \cdots p_t^{\alpha_t} q_1^{\gamma_1} \cdots q_u^{\gamma_u}$ and $k = p_1^{\beta_1} \cdots p_t^{\beta_t} \times s_1^{\omega_1} \cdots s_v^{\omega_v}$, where $q_i \neq s_j$. Define $r\langle k \rangle = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ with $r\langle k \rangle = 1$, if g.c.d. $(r,k)=1$. Let $\alpha \in S_n$ be of cycle-type $(j_1, \ldots, j_n)$. Then (2) has a solution if and only if $r\langle k \rangle$ divides j_k for each $k=1, \ldots, n$.

Correspondence to: William W. Chernoff, Department of Mathematics and Statistics, University of New Brunswick, Fredericton, N.B., Canada E3B 5A3.

SSDI 0012-365X(92)00189-9

It follows that a permutation $\alpha\in S_n$ has a p^l-th root if and only if its j_k's are such that

$$j_k \equiv 0 \bmod p^l \quad \text{if } k \equiv 0 \bmod p. \tag{3}$$

Thus, to enumerate the permutations in S_n with p^l-th roots, it is necessary to count all the permutations which satisfy condition (3).

It is convenient to consider a more general case, i.e. one where the permutations satisfy condition (1).

2. A theorem

The cycle index of the symmetric group S_t, see [7], denoted by $Z(S_t)$, is the polynomial in the variables $x_1,\dots,x_t$ defined as

$$Z(S_t)=\sum_{(i)}\left(\prod_{k=1}^{t}\frac{x_k^{i_k}}{k^{i_k}(i_k)!}\right), \tag{4}$$

where (i) denotes summation over all non-negative integral t-tuples $(i_1,\dots,i_t)$ such that $\sum_{k=1}^{t} ki_k=t$. Let $(1/n!)B_d^s(n)$, $n=dst$, $t\in\{0\}\cup Z^+$, be the polynomial in the variables $x_d, x_{2d},\dots,x_{td}$, obtained from (4) by replacing k by kd, x_k by x_{kd}, and i_k by si_k, i.e.

$$\frac{1}{n!}B_d^s(n)=\sum_{(i)}\left(\prod_{k=1}^{t}\frac{x_{kd}^{si_k}}{(kd)^{si_k}(si_k)!}\right).$$

When $n\not\equiv 0 \bmod ds$, let $B_d^s(n)=0$. One may readily check that $B_d^s(n)$ is a generating polynomial which enumerates, according to cycle type, the permutations in S_n of type $(j_1,\dots,j_n)$, where

$$j_k\equiv 0 \bmod s \quad \text{if } k\equiv 0 \bmod d,$$

and

$$j_k=0 \quad \text{if } k\not\equiv 0 \bmod d.$$

Let $A_d(n)$ be the generating polynomial in the variables x_j, $j\leqslant n$ and $j\not\equiv 0 \bmod d$, which enumerates, according to cycle type, the permutations in S_n of type $(j_1,\dots,j_n)$, where

$$j_k=0 \quad \text{if } k\equiv 0 \bmod d.$$

For convenience we set $A_d(0)=B_d^s(0)=1$. It follows that the polynomial

$$\sum_{t=0}^{\lfloor (n/ds)\rfloor}\binom{n}{dst}A_d(n-dst)B_d^s(dst) \tag{5}$$

enumerates, according to cycle type, the permutations in S_n which satisfy condition (1).

For the case $s=1$, (5) reduces to

$$\sum_{t=0}^{\lfloor (n/d)\rfloor}\binom{n}{dt}A_d(n-dt)B_d^1(dt)=n!\,Z(S_n).$$

Then by applying this to each term of the recurrence relation, see [6],

$$Z(S_n)=n^{-1}\sum_{j=1}^{n} x_j Z(S_{n-j}),$$

we get

$$A_d(n)=\sum_{j=1}^{n}\frac{(n-1)!}{(n-j)!}\delta_j x_j A_d(n-j), \tag{6}$$

where

$$\delta_j=\begin{cases}1 & \text{if } d \text{ does not divide } j,\\ 0 & \text{if } d \text{ divides } j,\end{cases}$$

and also

$$B_d^1(n)=\sum_{j=1}^{n/d}\frac{(n-1)!}{(n-dj)!}x_{dj}B_d^1(n-dj), \tag{7}$$

where $n\equiv 0 \bmod d$. Of course, when $n\not\equiv 0 \bmod d$, then $B_d^1(n)=0$.

We were not successful in finding a recurrence relation for $B_d^s(n)$ when $s>1$, and leave this as a problem for the reader.

Let $a_d(n)$ and $b_d^s(n)$ be the coefficient sums of $A_d(n)$ and $B_d^s(n)$, respectively, with $a_d(0)=b_d^s(0)=1$. In [4], Bolker and Gleason give direct counts for $a_d(n)$ and $b_d^1(n)$. They show that

$$a_d(n)=\prod_{j=1}^{n}(j-\theta_d(j)), \tag{8}$$

and that

$$b_d^1(n)=\prod_{j=1}^{n}(n-j+\theta_d(j)),$$

where

$$\theta_d(j)=\begin{cases}1 & \text{if } d \text{ divides } j,\\ 0 & \text{if } d \text{ does not divide } j.\end{cases}$$

In addition, as immediate consequences of (6) and (7), we have recurrence relations for $a_d(n)$ and $b_d^1(n)$. These are

$$a_d(n)=\sum_{j=1}^{n}\frac{(n-1)!}{(n-j)!}\delta_j a_d(n-j), \tag{9}$$

and

$$b_d^1(n)=\sum_{j=0}^{(n/d)-1}\frac{(n-1)!}{(dj)!}b_d^1(dj).$$

We note that the recurrence relation (9) is also given in [2].

To our knowledge, neither a direct count nor a recurrence relation has yet been found for $b_d^s(n)$ when $s>1$. We leave this as another problem for the reader.

Theorem 2.1. *Let $f_{d,s}(n)$, $d,s\in Z^+$, be the number of permutations in S_n of cycle type $(j_1,\dots,j_n)$, where $j_k\equiv 0 \bmod s$ if $k\equiv 0 \bmod d$. Then*

$$f_{d,s}(n)=\sum_{t=0}^{\lfloor (n/ds)\rfloor}\binom{n}{dst}a_d(n-dst)\,b_d^s(dst).$$

Proof. The result follows from (5). $\square$

Corollary 2.2. *If $n\not\equiv 0 \bmod d$, then $f_{d,s}(n)=nf_{d,s}(n-1)$.*

Proof. From (8) we have

$$a_d(n)=\begin{cases} na_d(n-1) & \text{if } n\not\equiv 0 \bmod d,\\ (n-1)a_d(n-1) & \text{if } n\equiv 0 \bmod d.\end{cases}$$

Then, if $n\not\equiv 0 \bmod d$,

$$\binom{n}{dst}a_d(n-dst)=n\binom{n-1}{dst}a_d(n-1-dst),$$

for each $t=0,\dots,\lfloor (n/ds)\rfloor$. The result follows. $\square$

Corollary 2.3. *If $n<ds$, then $f_{d,s}(n)=\prod_{j=1}^{n}(j-\theta_d(j))$.*

Proof. Follows by Theorem 2.1 and (8). $\square$

We know that $f_{d,s}(n)$, for the case $d=p$, a prime, and $s=p^l, l\in Z^+$, is the number of permutations in S_n with p^l-th roots. The following corollaries are then immediate consequences of the above results.

Corollary 2.4. *The number of permutations in S_n with p^l-th roots, p a prime, $l\in Z^+$, is*

$$f_{p,p^l}(n)=\sum_{t=0}^{\lfloor n/p^{l+1}\rfloor}\binom{n}{p^{l+1}t}a_p(n-p^{l+1}t)\,b_p^{p^l}(p^{l+1}t).$$

Corollary 2.5. *If $n\not\equiv 0 \bmod p$, then $f_{p,p^l}(n)=nf_{p,p^l}(n-1)$.*

For the case $p=2$, $l=1$, this reduces to $f_{2,2}(2k+1)=(2k+1)f_{2,2}(2k)$, a result given by Blum in [3].

Corollary 2.6. *If $n<p^{l+1}$, then $f_{p,p^l}(n)=\prod_{j=1}^{n}(j-\theta_p(j))$.*

Corollary 2.7. *If $n<p$, then $f_{p,p^l}(n)=n!$*

References

[1] E.A. Bender, Asymptotic methods in enumeration, SIAM Rev. 16 (1974) 485–515.
[2] E.A. Bertram and B. Gordon, Counting special permutations, European J. Combin. 10 (1989) 221–226.
[3] J. Blum, Enumeration of the square permutations in S_n, J. Combin. Theory Ser. A 17 (1974) 156–161.
[4] E.D. Bolker and A.M. Gleason, Counting permutations, J. Combin. Theory Ser. A 29 (1980) 236–242.
[5] I.Z. Bouwer and W.W. Chernoff, Solutions to $x^r = \alpha$ in the symmetric group, Ars Combin. 20 (1985) 83–88.
[6] F. Harary and E.M. Palmer, Graphical Enumeration (Academic Press, New York, 1973).
[7] J. Riordan, An Introduction to Combinatorial Analysis (Wiley, New York, 1958).